

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-331166  
(43)Date of publication of application : 30.11.2000

(51)Int.Cl. G06T 7/00  
H04L 9/32

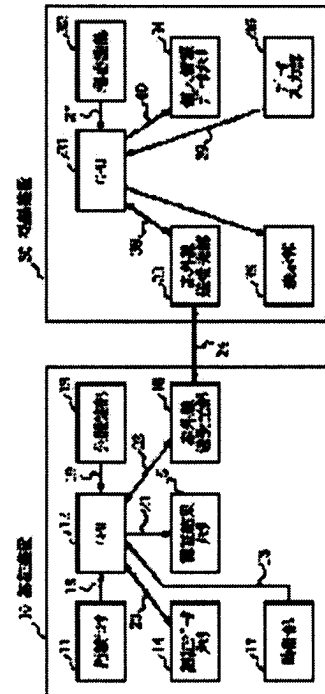
(21)Application number : 11-143578 (71)Applicant : NEC YONEZAWA LTD  
(22)Date of filing : 24.05.1999 (72)Inventor : YAMAZAKI ATSUSHI

## (54) FINGER PRINT AUTHENTICATING SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a finger print authenticating system where a highly safe simple system constitution is realized which does not allow the disclosure of finger print information.

**SOLUTION:** In this finger print authenticating system, a finger print sensor 11 detects finger prints and a public key section 13 stores a public key 19 used for encipherment. An authenticating data memory 14 stores authenticating data 20. An authenticating result memory 15 stores collating data 21 and a CPU 12 outputs the collating data 21 and authenticated and registered finger print data 22. A clock section 17 outputs time data 23 and a data inputting section 35 outputs personal information 39. A personal information data memory 34 stores personal information data 40 and a secret key section 32 stores secret keys 37 for encipherment and decoding. A displaying section 36 displays data and a CPU 31 manages and controls a registering device 30 and infrared-ray transmitting and receiving sections 16 and 33 transmit and receive infrared rays 24.



## LEGAL STATUS

[Date of request for examination] 26.04.2000

[Date of sending the examiner's decision of rejection] 10.06.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-331166  
(P2000-331166A)

(43) 公開日 平成12年11月30日 (2000. 11. 30)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テームコード\* (参考)

G 0 6 T 7/00

G 0 6 F 15/62

4 6 0 5 B 0 4 3

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 D 5 J 1 0 4

6 7 3 A

審査請求 有 請求項の数 6 O L (全 7 頁)

(21) 出願番号

特願平11-143578

(22) 出願日

平成11年5月24日 (1999. 5. 24)

(71) 出願人 000240617

米沢日本電気株式会社

山形県米沢市下花沢2丁目6番80号

(72) 発明者 山崎 敦

山形県米沢市下花沢2丁目6番80号 米沢

日本電気株式会社内

(74) 代理人 100082935

弁理士 京本 直樹 (外2名)

Fターム(参考) 5B043 AA01 AA04 BA02 CA08 CA10

FA03 FA07 HA20

5J104 AA07 EA19 GA03 KA01 KA05

KA17 MA02 NA02 NA05 NA36

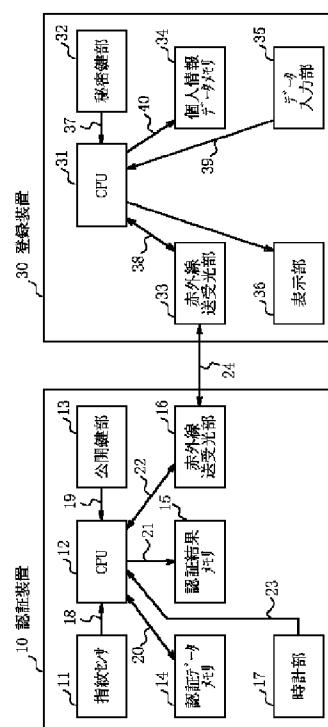
NA37 NA38 PA10 PA16

(54) 【発明の名称】 指紋認証システム

(57) 【要約】

【課題】 指紋情報を漏洩させない高度な安全性を簡単なシステム構成で実現する指紋認証システムを提供する。

【解決手段】 指紋センサ11は指紋を検出する。公開鍵部13は暗号化のための公開鍵19を格納する。認証データメモリ14は認証データ20を格納する。認証結果メモリ15は照合データ21を格納する。CPU12は照合データ21および認証登録指紋データ22を出力する。時計部17は時刻データ23を出力する。データ入力部35は個人情報39を出力する。個人情報データメモリ34は個人情報データ40を格納する。秘密鍵部32は暗号化および復号化のための秘密鍵37を格納する。表示部36はデータを表示する。CPU31は登録装置30の管理制御を行う。赤外線送受光部16、33は赤外光24を送受する。



【特許請求の範囲】

【請求項1】 指紋情報を暗号化し予め認証登録指紋データとして送信し、指紋照合時に指紋センサデータと、受信及び格納した認証データを復号しこれと比較照合することにより認証を行う認証装置と；前記認証装置から受信した前記認証登録指紋データを復号し、これと個人情報データとから認証データの生成及び暗号化を行い、前記認証データとして送信する登録装置と；を備えたことを特徴とする指紋認証システム。

【請求項2】 前記認証装置が、指紋を検出し指紋情報を出力する指紋センサと；前記指紋情報の暗号化のための公開鍵を格納する公開鍵部と；前記認証データを格納する認証データメモリと；前記指紋情報と前記認証データとを比較照合した照合データを格納する認証結果メモリと；時刻データを出力する時計部と；前記指紋情報の暗号化、前記認証データの復号化、これらを照合し前記照合データ及び前記認証登録指紋データを出力する第1のマイクロプロセッサと；前記認証登録指紋データの送受を赤外線により行う第1の赤外線送受光部と；を有することを特徴とする請求項1記載の指紋認証システム。

【請求項3】 前記登録装置が、前記赤外線を送受する第2の赤外線送受光部と；データ入力を行い個人情報を出力するデータ入力部と；前記個人情報データを格納する個人情報データメモリと；暗号化及び復号化のための秘密鍵を格納する秘密鍵部と；データの表示を行う表示部と；復号化した前記認証登録指紋データ及び前記個人情報データから前記認証データを生成し、これを暗号化する第2のマイクロプロセッサと；を有することを特徴とする請求項1又は請求項2記載の指紋認証システム。

【請求項4】 前記認証装置及び前記登録装置間の送受信通信をイーサネット（登録商標）により行うことを特徴とする請求項1、2又は3記載の指紋認証システム。

【請求項5】 前記認証装置が、第1のマイクロプロセッサと、前記指紋センサと、作業用メモリと、時刻データを出力する時計と、赤外線送受光器と、プログラム及び各種データを記憶する不揮発性メモリと、電源供給の電池と、カバーオープン検出回路とを有することを特徴とする請求項1記載の指紋認証システム。

【請求項6】 前記作業用メモリが、フラッシュ・リード・オンリー・メモリであることを特徴とする請求項5記載の指紋認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は指紋認証システムに関し、特に指紋情報を予め登録した認証データと照合する指紋認証システムに関する。

【0002】

【従来の技術】 一般に、金融機関や防衛施設等では高度なセキュリティ管理が要求されるので、予め登録された人物に対してのみ金融利用や入室等の許可を行う個人指紋認識システムが広く用いられている。

【0003】 個人の指紋パターンは、隆線が分岐する位置と分岐数、終端する位置が個人により異なる特徴を有するので、この特徴を抽出して指紋情報の判定を行うことができる。

【0004】 図4は従来の指紋認証システムを示すブロック図である。

【0005】 従来の指紋認証システムは、指紋を検出する指紋センサ1と、個人情報のデータを入力するデータ入力部4と、個人情報のデータを表示する表示部5と、個人情報のデータを記憶する個人情報データ記憶部3と、データの管理制御を行うCPU2と、CPU2により処理された指紋の照合結果を記憶する認証結果メモリ6とから構成されている。

【0006】 次に動作について説明する。

【0007】 指紋センサ1は指紋を数値データに変換し、指紋データとしてCPU2に出力する。CPU2は、個人情報データ記憶部3に記憶していた指紋データと指紋センサ1から読みとった指紋データとを比較し本人照合を行い、照合結果を認証結果メモリ6に格納する。

【0008】 データ入力部4と表示部5は、個人情報の入力と画面表示に使用される。

【0009】 この構成の場合、個人情報を暗号化することも可能であるが、暗号化、復号化に使用する鍵データは、両方とも指紋認証システム内に組み込む必要がある。

【0010】 このような技術の一例として、特開平5-290149号公報記載の「指紋照合認証方式及びその装置」が知られている。

【0011】 この公報では、指紋照合に用いる指紋情報を暗号化して登録し、かつ照合時にも暗号化したままの状態では照合することで、指紋のオリジナル情報が盗まれたり漏洩することを防止する技術が記載されている。

【0012】

【発明が解決しようとする課題】 上述した従来の指紋認証システムは、個別に個人情報を登録する必要があるため、システム構成が複雑になるという欠点を有している。

【0013】 個人情報が指紋認証システムに格納されているため、指紋認証システムを解析すれば偽装が可能になり指紋情報が漏洩するという欠点を有している。

【0014】 また、個人情報を暗号化して格納する場合でも、暗号化と復号化に使用する鍵は、指紋認証システム内に格納するため、暗号解読が可能であり指紋情報が漏洩するという欠点を有している。

【0015】 本発明の目的は、指紋情報を漏洩させない

高度な安全性を簡単なシステム構成で実現する指紋認証システムを提供することにある。

#### 【0016】

【課題を解決するための手段】本発明の指紋認証システムは、指紋情報を暗号化し予め認証登録指紋データとして送信し、指紋照合時に指紋センサデータと、受信及び格納した認証データを復号しこれと比較照合することにより認証を行う認証装置と；前記認証装置から受信した前記認証登録指紋データを復号し、これと個人情報データとから認証データの生成及び暗号化を行い、前記認証データとして送信する登録装置と；を備えたことを特徴としている。

【0017】前記認証装置が、指紋を検出し指紋情報を出力する指紋センサと；前記指紋情報の暗号化のための公開鍵を格納する公開鍵部と；前記認証データを格納する認証データメモリと；前記指紋情報と前記認証データとを比較照合した照合データを格納する認証結果メモリと；時刻データを出力する時計部と；前記指紋情報の暗号化、前記認証データの復号化、これらを照合し前記照合データ及び前記認証登録指紋データを出力する第1のマイクロプロセッサと；前記認証登録指紋データの送受を赤外光により行う第1の赤外線送受光部と；を有することを特徴としている。

【0018】前記登録装置が、前記赤外光を送受する第2の赤外線送受光部と；データ入力を行い個人情報を出力するデータ入力部と；前記個人情報データを格納する個人情報データメモリと；暗号化及び復号化のための秘密鍵を格納する秘密鍵部と；データの表示を行う表示部と；復号化した前記認証登録指紋データ及び前記個人情報データから前記認証データを生成し、これを暗号化する第2のマイクロプロセッサと；を有することを特徴としている。

【0019】また、前記認証装置及び前記登録装置間の送受信通信をイーサネットにより行うことを特徴としている。

【0020】前記認証装置が、第1のマイクロプロセッサと、前記指紋センサと、作業用メモリと、時刻データを出力する時計と、赤外線送受光器と、プログラム及び各種データを記憶する不揮発性メモリと、電源供給の電池と、カバーオープン検出回路とを有することを特徴としている。

【0021】前記作業用メモリが、フラッシュ・リード・オンリー・メモリであることを特徴としている。

#### 【0022】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0023】図1は本発明の指紋認証システムの一つの実施の形態を示すブロック図である。

【0024】図1に示す本実施の形態は、指紋認証を行う認証装置10と、指紋データや個人データの登録を行

う登録装置30とから構成されている。

【0025】認証装置10は指紋を検出し指紋情報18を出力する指紋センサ11と、指紋情報18の暗号化のための公開鍵19を格納する公開鍵部13と、認証データ20を格納する認証データメモリ14と、指紋情報18および認証データ20を比較照合した照合データ21を格納する認証結果メモリ15と、時刻データ23を出力する時計部17と、指紋情報18の暗号化、認証データ20の復号化、これらを照合し照合データ21および認証登録指紋データ22を出力するCPU12と、認証登録指紋データ22の送受を赤外光24により行う赤外線送受光部16とを有している。

【0026】また、登録装置30は赤外光24を送受する赤外線送受光部33と、データ入力を行い個人情報39を出力するデータ入力部35と、個人情報データ40を格納する個人情報データメモリ34と、暗号化および復号化のための秘密鍵37を格納する秘密鍵部32と、データの表示を行う表示部36と、認証登録指紋データ22を復号化しこれを個人情報データ40とから認証データ38を生成し、暗号化するCPU31とを有している。

【0027】ここで公開鍵、秘密鍵とは数値データであり、生成多項式により生成される暗号データである。一般に、公開鍵で暗号化したデータは秘密鍵でのみ復号化でき、逆に秘密鍵で暗号化されたデータは公開鍵でのみ復号化できる特性を有しているため、漏洩に対する安全性が高い。これら公開鍵、秘密鍵のデータは個別素子に格納されると云うよりは、プログラムメモリの一部に格納される。

【0028】公開鍵19、秘密鍵37を使った暗号化方式の特徴を説明すると、鍵と呼ばれている物は、暗号化、復号化するための数値データである。公開鍵暗号化方式とは、公開鍵で暗号化したデータは秘密鍵でのみ復号化可能で、同様に秘密鍵で暗号化したデータは公開鍵でのみ復号化できる方式を云う。この特徴を利用して、安全にかつ簡単な構成で認証システムが構築可能となる。

【0029】次に各部の動作を説明する。

【0030】指紋センサ11は個人の指紋を数値化し指紋情報18を出力する。CPU12は認証データメモリ14が格納する認証データ20を読み出し、公開鍵19で復号化した後指紋情報18と比較し、比較した結果をさらに公開鍵19で暗号化し、照合データ21として認証結果メモリ15に格納する。

【0031】このとき、時計部17から得られる時刻データ23も同時に公開鍵19で暗号化して認証結果メモリ15に格納する。認証データ20の登録は、認証装置10の赤外線送受光部16と登録装置30の赤外線送受光部33を使って相互に通信することにより行う。

【0032】まず、データ入力部35から入力された個

個人情報39を、表示部36で確認する。同時に、認証装置10の指紋センサ11で指紋を読み込ませ、公開鍵部13に格納された公開鍵19で暗号化した認証登録指紋データ22を、赤外線送受光部16で赤外光24により登録装置30へ送信する。

【0033】登録装置30は、秘密鍵部32に格納した秘密鍵37で復号化し、入力した個人情報39と認証登録指紋データ22とを併せてこれらを個人情報データ40として、個人情報データメモリ34に格納する。同時に、個人情報39と認証登録指紋データ22を基にして認証データ38を生成し、秘密鍵部32の秘密鍵37で暗号化した後、赤外線送受光部33を使って認証装置10に送信する。この受信された認証データ38は、CPU12により処理され認証データ20として認証データメモリ14に格納される。

【0034】図2は本発明の指紋認証システムの動作の一例を示す動作説明図であり、図2(a)は認証動作を示し、図2(b)は登録動作を示す。

【0035】次に、図1および図2(a)を参照して本実施の形態の動作をより詳細に説明する。

【0036】指が指紋センサ11に置かれると、指紋センサ11は指の指紋を数値化し指紋情報18として出力する。

【0037】ここで指紋の数値化とは、指紋と一对一の数値データに置き換えることを意味するが、人間の指紋のパターン(右巻き、左巻き)と任意の何点かの特徴点とを抽出し、データパターン化している。

【0038】認証データメモリ14に格納された認証データ20を公開鍵19で復号化し、読みとった指紋情報18と比較する。比較した照合結果は照合データ21として、時刻データ23と共に公開鍵19で暗号化され認証結果メモリ15に格納される。なお、入室システムに利用する場合は、照合結果により扉を開放する。認証結果の記録は、登録装置30を使って確認できる。

【0039】次に登録動作を図2(b)を使用して説明する。

【0040】ここで、認証装置10と登録装置30の赤外線送受光部16、33が赤外光24で通信できる状態とする。

【0041】データ入力部35を用いて個人情報39を入力する。同時に、認証装置10の指紋センサ11で登録する人の指紋を読み込ませる。認証装置10側で、公開鍵19を使い指紋情報18を暗号化して、登録装置30に送信する。登録装置30では指紋情報18を含む認証登録指紋データ22を秘密鍵37で復号化して、入力された個人情報39と併せて個人情報データメモリ34に格納する。

【0042】同時に、認証データ38を作成し、秘密鍵37で暗号化し認証装置10へ送信する。認証装置10は、認証データ20を認証データメモリ14へ格納す

る。

【0043】このとき、秘密鍵37を替えることにより、複数の認証データ38を生成できる。

【0044】なお、認証データについて説明すると、登録装置30に登録されている個人情報データ40は、個人を識別する情報(例えば、名前、社員番号等)と、個人に対する指紋情報18と、個人が保有する権利の種別(どの認証システムで認証されるか、例えば入室システムの場合は入室権)とから構成されている。これに対して、認証装置10に暗号化されて格納される認証データ20は、指紋情報18と、この認証装置10における権利からのみ構成されているので、たとえ認証データ20を解析できても、個人を特定することができず、偽装は困難となる。

【0045】図3は図1に示す認証装置の詳細ブロック図である。

【0046】なお、図3において図1に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【0047】図3を参照すると、認証装置10はCPU12と、指紋センサ11と、作業用メモリ25と、時刻データ23を出力する時計26と、赤外線送受光器27と、プログラムおよび各種データを記憶する不揮発性メモリ28と、電源供給の電池7と、カバーオープン検出回路8とから構成され、筐体(図示せず)に収容される。

【0048】不揮発性メモリ28として例えばフラッシュROMが使用され、CPU12の動作プログラム、指紋認証プログラム、公開鍵または秘密鍵のデータ、暗号化された指紋データ、認証結果のログ(記録)が格納されている。フラッシュROMは電源オフ状態でも格納したデータを保持するが、特別なプログラム操作で消去、書き換えが可能である。指紋センサ11は指紋を指紋画像データとして数値化して読み込む。CPU12は指紋画像データをバス29を介して作業用メモリ25に蓄積してから、不揮発性メモリ28の指紋認証プログラムを起動する。ここで暗号化された指紋画像データを公開鍵19で復号し、作業用メモリ25に予め蓄積した指紋画像データと比較する。

【0049】この比較結果は認証されても認証されなくても、時計26の時刻データとともに暗号化されて認証結果のログとして不揮発性メモリ28に記録される。赤外線送受光器27経由で、登録装置30からの要求があれば、認証結果のログの送信、指紋画像データの更新、公開鍵の更新等を行う。

【0050】なお、外部電源(図示せず)が切断されると指紋認証は行わないが、一定時間動作する電池7により電力を供給する。筐体のカバーが開けられた場合、カバーオープン検出回路8が作動し、カバーオープンを示すカバー検出信号9をCPU12に出力する。CPU1

2は、外部電源が切断されていても電池7で動作できるので、不揮発性メモリ28の公開鍵データを消去することができる。このため、公開鍵データの漏洩を防ぐことができる。

【0051】なお、認証装置10と登録装置30との通信は赤外線送受光部16、33による赤外線通信に限定されるものではなく、イーサネットをもちいた通信でもよい。

【0052】上述の通り、認証装置10には暗号化された認証データ20と公開鍵19とが格納されているだけであるので、秘密鍵37がないと復号できないため個人情報情報が安全に保護され、認証装置10も簡単な構成で実現できる。

【0053】

【発明の効果】以上説明したように、本発明の指紋認証システムは認証装置と登録装置とが分離しておりシステム構成を簡素化できるので、1台の登録装置で複数の認証装置を管理できるという効果を有している。

【0054】認証装置には個人情報情報を格納せず暗号化された認証データのみを格納し、かつ認証データを生成する秘密鍵を有さないので、認証データの偽造を防止できるという効果を有している。

【0055】また、認証装置と登録装置の通信は全て暗号化しているので、安全性を確保できるという効果を有している。

【図面の簡単な説明】

【図1】本発明の指紋認証システムの一つの実施の形態を示すブロック図である。

【図2】本発明の指紋認証システムの動作の一例を示す動作説明図である。

【図3】図1に示す認証装置の詳細ブロック図である。

【図4】従来の指紋認証システムを示すブロック図である。

【符号の説明】

1 指紋センサ

2 CPU

3 個人情報データ記憶部

4 データ入力部

5 表示部

6 認証結果メモリ

7 電池

8 カバーオープン検出回路

9 カバー検出信号

10 認証装置

11 指紋センサ

12 CPU

13 公開鍵部

14 認証データメモリ

15 認証結果メモリ

16 赤外線送受光部

17 時計部

18 指紋情報

19 公開鍵

20 認証データ

21 照合データ

22 認証登録指紋データ

23 時刻データ

24 赤外光

25 作業用メモリ

26 時計

27 赤外線送受光器

28 不揮発性メモリ

29 バス

30 登録装置

31 CPU

32 秘密鍵部

33 赤外線送受光部

34 個人情報データメモリ

35 データ入力部

36 表示部

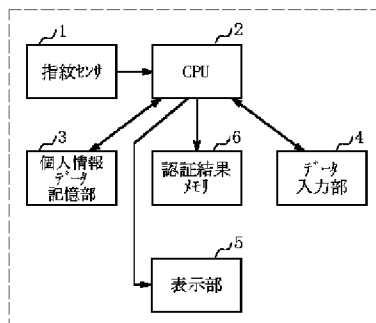
37 秘密鍵

38 認証データ

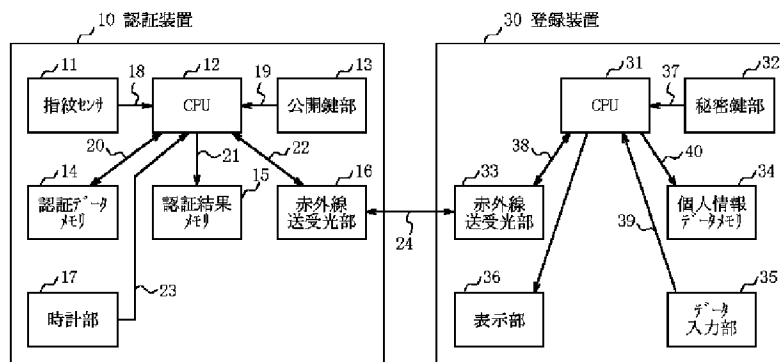
39 個人情報

40 個人情報データ

【図4】

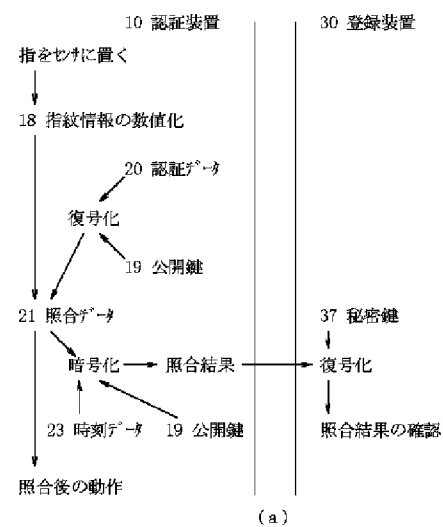


【図 1】

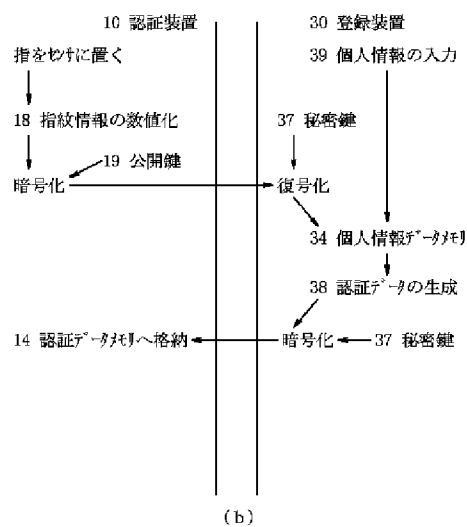


【図 2】

<認証動作>



<登録動作>



【図3】

